Les nombres p-adiques

Ahmet Emin TATAR

1 Introduction

Dans ce mémoire, nous allons déterminer toutes les valeurs absolues sur le corps $\mathbb{Q}$ et nous allons essayer de compléter $\mathbb{Q}$ par ces valeurs absolues. Finalement, nous donnerons une procédure générale pour les corps valués ultra-métriques.

On sait que le corps de nombres réels $\mathbb{R}$ est complété de $\mathbb{Q}$ pour la valeur absolue et qu'à chaque nombre premier p on peut associer une valeur absolue (que l'on appelle valeur absolue p-adique). Les questions que l'on se pose est:

- Est ce qu'il y a d'autres valeurs absolues sur $\mathbb{Q}$?
- Si oui, quels sont les autres complétés de $\mathbb{Q}$ pour ces valeurs absolues?

La première partie de ce mémoire tentera de répondre à la première question. Quant à la seconde question, elle sera abordée dans la deuxième partie.

Dans la première partie, nous allons commencer par entiers p-adiques, puis nous allons construire respectivement l'anneau des entiers p-adiques $\mathbb{Z}_p$, et le corps des nombres p-adiques $\mathbb{Q}_p$. Ensuite, nous définirons la topologie p-adique (la topologie définie par la valeur absolue p-adique) sur $\mathbb{Q}_p$. Nous étudierons alors le théorème d'Ostrowski qui dit que la valeur absolue p-adique et ordinaire forment toutes les valeurs absolues qu'on peut considérer sur $\mathbb{Q}$. Nous clorons cette première partie en parlant des valeurs absolues sur le corps de nombres, et nous verrons que sur ce corps de degrés n où $n = r + 2s$ on peut définir $r + s$ valeurs absolues non équivalentes induisant la topologie réelle sur $\mathbb{Q}$ (de même pour celle qui induisent la topologie p-adique sur $\mathbb{Q}$). Pour cela, nous auront besoin de nouvelles notions comme: anneau de Dedekind, idéal fractionnaire, norme d'un idéal qui seront détaillées dans la partie annexe.

La seconde partie, qui traite donc la deuxième question posée, sera au sujet des valeurs absolues ultra-métriques et des corps ultra-métriques, leurs propriétés métriques et la procédure générale de complété d'un corps ultra-métrique. Comme cas particulier, nous parlerons de la valeur absolue p-adique et $\mathbb{Q}_p$.

2 Partie I

2.1 Entiers p-adiques et $\mathbb{Z}_p$

Pour tout $x \in \mathbb{Z}$ on sait définir son développement de Hensel fini.

$$x = \sum_{i=1}^n x_i p^i \text{ avec } x_i \in \{0, \dots, p-1\}$$

Mais comment définir un développement de Hensel infini?

Definition 1 (Entiers p-adiques et $\mathbb{Z}_p$). On définit un entier p-adique comme une suite $(x_n)_{n \geq 1}$ vérifiant $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ avec

$$\begin{aligned} \mathbb{Z}/p^{n+1}\mathbb{Z} &\hookrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ x_{n+1} &\longrightarrow x_n \end{aligned}$$

On appelle l'ensemble des entiers p-adiques $\mathbb{Z}_p$. $\mathbb{Z}_p$ est un anneau pour les opérations arithmétiques sur les séries.

Soit $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ alors x_n est une classe. On note a_n sa représentante. Alors a_n est un entier tel que $0 \leq a_n < p^n$. a_n a un développement de Hensel fini, alors a_n s'écrit

$$a_n = \sum_{k=0}^n b_k p^k \text{ avec } b_k \in \{0, \dots, p-1\}$$

Propriété 1. Soit $x \in \mathbb{Z}_p$. Il existe une unique suite $(b_n)_{n \geq 0}$ avec $0 \leq b_n < p$ tel que la série

$$\sum_{n \geq 0} b_n p^n \text{ converge vers } x$$

Cette série est appelée développement de Hensel infini de x .

Proof. :

- *Existence du développement de Hensel:* Soit $x = (x_n)_{n \geq 1} \in \mathbb{Z}_p$. On représente x par la suite $(a_n)_{n \geq 1}$ tel que $\forall n \in \mathbb{N}$, $a_n \in \mathbb{Z}/p^n\mathbb{Z}$. Alors a_n admet un développement de Hensel fini. $a_n = b_0 + b_1 p + \dots + b_n p^n$. Comme $x \in \mathbb{Z}_p$ on a $\forall n \geq 1$, $p^n | a_{n+1} - a_n$, d'où a_{n+1} s'écrit aussi sous la forme $a_{n+1} = b_0 + b_1 p + \dots + b_n p^n + b_{n+1} p^{n+1}$. Or la série $\sum b_k p^k$ est convergente et converge vers x . On appelle cette limite le développement de Hensel de x .
- *Unicité du développement de Hensel:* Supposons, par l'absurde, que x admet deux développements de Hensel différents. Alors, il existe deux suites $(x_k)_{k \geq 0}$ et $(y_k)_{k \geq 0}$ tel que

$$x = \sum_{k \geq 0} x_k p^k = \sum_{k \geq 0} y_k p^k$$

et il existe k_0 $y_{k_0} \neq x_{k_0}$. On considère l'ensemble $N = \{k \in \mathbb{N} / x_k \neq y_k\}$. Par hypothèse, $N \neq \emptyset$ et $N \subset \mathbb{N}$ alors N admet un minimum. Soit k' ce minimum, alors $\forall k < k'$ $x_k = y_k \Rightarrow \nu(x_k - y_k) = k'$. On pose

$$x' = \sum_{k \geq 0} (x_k - y_k) p^k$$

D'une part, $x' = 0$ car

$$\sum_{k \geq 0} x_k p^k = \sum_{k \geq 0} y_k p^k$$

D'autre part,

$$x' = \sum_{k \geq k'} (x_k - y_k) p^k = 0$$

D'où, $\forall n \in \mathbb{N}$, $p^{k'+n} | x' \Rightarrow \nu(x_k - y_k) \geq k' + n$. Ceci contredit la minimalité de k' .

□

2.2 Valuation de $\mathbb{Z}_p$

Soit $a \in \mathbb{Z}_p$, alors

$$a = \sum_{n \geq 0} a_n p^n \text{ est son développement de Hensel.}$$

On définit une suite de morphisme π_n tel que

$$\begin{aligned} \pi_n : \mathbb{Z}_p &\mapsto \mathbb{Z}/p^n\mathbb{Z}, & \forall n \geq 0 \\ x &\longmapsto a_n \end{aligned}$$

Definition 2 (Valuation p-adique). La valuation p-adique est une fonction de $\mathbb{Z}_p$ dans $\mathbb{N} \cup \{+\infty\}$ vérifiant:

$$\forall a \in \mathbb{Z}_p \begin{cases} \nu(a) = \inf\{n/a_n \neq 0\} = \sup\{n/p^n | a\}, \text{ si } a \neq 0 \\ \nu(0) = +\infty \end{cases}$$

Voici quelques propriétés de la valuation p-adique:

Propriété 2. Soit $a \in \mathbb{Z}_p$ alors les conditions suivantes sont équivalentes:

- i. a est une unité
- ii. $\Pi_0(a) \neq 0$
- iii. $\nu(a) = 0$

Proof. :

i. $\Rightarrow$ ii. On suppose que a est une unité dans $\mathbb{Z}_p$. Alors il existe $b \in \mathbb{Z}_p$ tel que $ab = 1$.
 $\Rightarrow \Pi_0(ab) = \Pi_0(a)\Pi_0(b) = \Pi_0(1) \neq 0$
 $\Rightarrow \Pi_0(a) = a_0 \neq 0$.

ii. $\Rightarrow$ iii. On suppose que $\Pi_0(a) \neq 0$ alors $a_0 \neq 0 \Rightarrow \nu(a) < 1 \Rightarrow \nu(a) = 0$

iii. $\Rightarrow$ i. On suppose que $\nu(a) = 0$. Alors $a_0 \neq 0$. a s'écrit $a = a_0 + a_1 p + a_2 p^2 + \dots$. Comme $a_0 \neq 0$, on réécrit a en facteur de a_0 . $a = a_0(1 + \frac{a_1}{a_0} p + \frac{a_2}{a_0} p^2 + \dots)$. D'où $a^{-1} = a_0^{-1}(1 + \frac{a_1}{a_0} p + \frac{a_2}{a_0} p^2 + \dots)^{-1}$. En posant $u = (1 + \frac{a_1}{a_0} p + \frac{a_2}{a_0} p^2 + \dots)$ et en utilisant le développement limité de $\frac{1}{1+u}$, on déduit que $a^{-1} = a_0^{-1}(1 - u + u^2 - u^3 + \dots)$. Il reste à montrer que $\forall n, u^n \in$

□

Propriété 3. La valuation p -adique vérifie:

i. $\forall x \in \mathbb{Z}_p, \nu(x) = +\infty \Leftrightarrow x = 0$

ii. $\forall x, y \in \mathbb{Z}_p, \nu(xy) = \nu(x) + \nu(y)$

iii. $\forall x, y \in \mathbb{Z}_p, \nu(x + y) \geq \inf(\nu(x), \nu(y))$

Proof. :

i. est évident par définition de ν

ii. Il y a trois cas à étudier:

Cas 1: Si $x = 0$ ou $y = 0$, on a $xy = 0$ donc $\nu(xy) = +\infty$ et $\nu(x) + \nu(y) = +\infty$ d'où l'égalité.

Cas 2: Si $xy \neq 0$ alors $\nu(xy) = +\infty$ c'est-à-dire $\forall n \in \mathbb{N}, p^n | xy \Rightarrow \forall k, m \in \mathbb{N}$ tel que $k + m = n, p^k | x$ et $p^m | y \Rightarrow k \leq \nu(x)$ et $m \leq \nu(y), \forall k, m$. Alors, $\nu(x) = +\infty$ ou $\nu(y) = +\infty$. Par la convention $+\infty + +\infty = +\infty$, on a $\nu(x) + \nu(y) = +\infty$. D'où l'égalité.

Cas 3: Soit $x, y \in \mathbb{Z}_p$ non nuls alors

$$x = \sum_{n \geq 0} x_n p^n, \quad y = \sum_{n \geq 0} y_n p^n$$

On suppose que $\nu(x) = k, \quad \nu(y) = m$

$$\nu(x) = k \Rightarrow a_i = 0, \forall i \leq k \Rightarrow x = \sum_{n \geq k} x_n p^n = p^k \sum_{n \geq 0} x_{n+k} p^n$$

On pose

$$x' = \sum_{n \geq 0} x_{n+k} p^n$$

alors $\nu(x') = 0$ et $x = x' p^k$

De même, y s'écrit

$$y = p^m \sum_{n \geq 0} x_{n+m} p^n y = y' p^m \text{ avec } \nu(y') = 0$$

D'après la propriété précédente:

$$\begin{cases} \nu(x') = 0 \Leftrightarrow \Pi_0(x') \neq 0 \\ \nu(y') = 0 \Leftrightarrow \Pi_0(y') \neq 0 \end{cases}$$

Mais Π_0 est un morphisme d'où:

$$\begin{aligned} & \Pi_0(x') \Pi_0(y') \neq 0 \\ \Rightarrow & \Pi_0(x' y') \neq 0 \\ \Rightarrow & \nu(x' y') \neq 0 \\ \Rightarrow & p \nmid x' y' \\ \Rightarrow & \nu(xy) = m + k = \sup\{n/p^n | xy\} \\ \Rightarrow & \nu(x + y) = \nu(x) + \nu(y) \end{aligned}$$

iii. Soit $x, y \in \mathbb{Z}_p$ alors

$$x = \sum_{n \geq 0} x_n p^n \text{ et } y = \sum_{n \geq 0} y_n p^n$$

On pose $k = \inf(\nu(x), \nu(y))$ alors $\nu(x) \geq k$ et $\nu(y) \geq k$

$$\Rightarrow x_i = y_i = 0, \forall i < k,$$

$$\Rightarrow x_i + y_i = 0, \forall i < k,$$

$$\Rightarrow p^k | x + y \Rightarrow \nu(x + y) \geq k$$

□

Propriété 4. Soient $x, y \in \mathbb{Z}_p$, si $\nu(x) \neq \nu(y)$ alors $\nu(x + y) = \inf(\nu(x), \nu(y))$.

Proof. Soient $x, y \in \mathbb{Z}_p$, alors

$$x = \sum_{n \geq 0} x_n p^n \text{ et } y = \sum_{n \geq 0} y_n p^n$$

On suppose que $\nu(x) \neq \nu(y)$. Pour fixer les idées, disons que $k = \nu(y) < \nu(x)$. Alors $x_k = 0$ et $y_k \neq 0$

$$\Rightarrow x_k + y_k \neq 0$$

$$\Rightarrow \nu(x + y) < k = \nu(y) = \inf(\nu(x), \nu(y))$$

Or, on a toujours $\nu(x + y) \geq \inf(\nu(x), \nu(y))$. Donc $\nu(x + y) = \inf(\nu(x), \nu(y))$. □

Propriété 5. L'anneau $\mathbb{Z}_p$ est intègre.

Proof. Soient $x, y \in \mathbb{Z}_p$, tel que $xy = 0$ alors $\nu(xy) = +\infty$, or $\nu(xy) = \nu(x) + \nu(y)$. D'où $\nu(x) + \nu(y) = +\infty$.

Cela implique $\nu(x) = +\infty$ ou $\nu(y) = +\infty$, on en déduit que $x = 0$ ou $y = 0$.

Donc, $\mathbb{Z}_p$ est intègre. □

Propriété 6. Soient $x, y \in \mathbb{Z}_p$, alors $x|y \Leftrightarrow \nu(x) \leq \nu(y)$.

Proof. Soient $x, y \in \mathbb{Z}_p$:

$\Rightarrow$ On suppose que $x|y$ dans $\mathbb{Z}_p$, alors $\exists z \in \mathbb{Z}_p$ tel que $y = xz$, d'où $\nu(y) = \nu(x) + \nu(z)$. Comme $\nu(x), \nu(z) \in \mathbb{N} \cup \{+\infty\}$, $\nu(y) \geq \nu(x)$.

$\Leftarrow$ On suppose que $\nu(x) \leq \nu(y)$. y s'écrit

$$y = \sum_{n \geq 0} y_n p^n = p^{\nu(y)} \sum_{n \geq 0} y_{n+\nu(y)} p^n = p^{\nu(y)} y'$$

avec

$$y' = \sum_{n \geq 0} y_{n+\nu(y)} p^n \text{ et } \nu(y') = 0$$

De même, x s'écrit $x = p^{\nu(x)} x'$ avec

$$x' = \sum_{n \geq 0} x_{n+\nu(x)} p^n \text{ et } \nu(x') = 0$$

$\nu(y') = 0 \Rightarrow y'$ inversible $\Rightarrow \exists c_1 \in \mathbb{Z}_p$ tel que $y'c_1 = 1 \Rightarrow yc_1 = p^{\nu(y)}$.
 De même, il existe $c_2 \in \mathbb{Z}_p$ tel que $xc_2 = p^{\nu(x)}$
 Comme $\nu(y) \geq \nu(x)$, $p^{\nu(x)} | p^{\nu(y)} \Rightarrow xc_2 | yc_1 \Rightarrow \exists c \in \mathbb{Z}_p$ tel que $yc_1 = xc_1c \Rightarrow x|y$.

□

2.3 Le corps $\mathbb{Q}_p$: Corps des nombres p-adiques

Definition 3 (Corps des nombres). *Un corps des nombres K est une extension de degré finie de $\mathbb{Q}$.*

Definition 4 (Corps des nombres p-adiques). *$\mathbb{Q}_p$ est le corps de fraction de $\mathbb{Z}_p$, c'est à dire*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} / a \in \mathbb{Z}_p \text{ et } b \in \mathbb{Z}_p^* \right\}.$$

Voici quelques propriétés de $\mathbb{Q}_p$.

Propriété 7. $\forall x \in \mathbb{Q}_p^*$ admet une unique représentation $x = p^n u$ où $n \in \mathbb{Z}$ et u est une unité dans $\mathbb{Z}_p$.

Proof. :

- *Existence de la représentation:* Soit $x \in \mathbb{Q}_p^*$ alors x s'écrit $x = \frac{a}{b}$ avec $a \in \mathbb{Z}_p$ et $b \in \mathbb{Z}_p \setminus \{0\}$. On sait que $a = a'p^k$ et $b = b'p^m$ avec a', b' unités dans $\mathbb{Z}_p$ et $k = \nu(a)$, $m = \nu(b)$ d'où

$$x = \frac{a'}{b'} p^{k-m}$$

- *Unicité de la représentation:* Supposons que $x \in \mathbb{Q}_p^*$ admet deux représentations. $x = up^k = vp^m$ avec u, v unités dans $\mathbb{Z}_p$ et $k, m \in \mathbb{Z}$. Alors,

$$uv^{-1} = p^{m-k} \Rightarrow \nu(uv^{-1}) = \nu(p^{m-k}) = m - k.$$

Or, $\nu(uv^{-1}) = 0$ car uv^{-1} est une unité. Ce qui implique $m = k$. D'où, l'unicité de la représentation.

□

Propriété 8. *La fonction ν définit sur $\mathbb{Q}_p$ dans $\mathbb{Z} \cup \{+\infty\}$ vérifiant*

$$\begin{cases} \forall x \in \mathbb{Q}_p \setminus \{0\}, x = p^{\nu(x)}u, \text{ où } u \text{ est une unité dans } \mathbb{Z}_p \\ \nu(0) = +\infty \end{cases}$$

est une valuation sur $\mathbb{Q}_p$.

Proof. On va montrer que $\nu : \mathbb{Q}_p \mapsto \mathbb{Z} \cup \{+\infty\}$ vérifie

- $\forall x \in \mathbb{Q}_p, \nu(x) = +\infty \Leftrightarrow x = 0$
- $\forall x, y \in \mathbb{Q}_p, \nu(xy) = \nu(x) + \nu(y)$
- $\forall x, y \in \mathbb{Q}_p, \nu(x + y) \geq \inf(\nu(x), \nu(y))$

i. est évidente par définition.

ii. Soient $x, y \in \mathbb{Q}_p$ alors x et y s'écrivent

$$\left. \begin{array}{l} x = up^k = up^{\nu(x)} \text{ avec } u \text{ unité dans } \mathbb{Z}_p \\ y = vp^m = vp^{\nu(y)} \text{ avec } v \text{ unité dans } \mathbb{Z}_p \end{array} \right\} xy = uvp^{k+m} = uvp^{\nu(x)+\nu(y)}$$

Or, $xy = u'p^{\nu(xy)}$ avec u' unité dans $\mathbb{Z}_p$.

L'unicité de l'écriture implique $\nu(xy) = \nu(x) + \nu(y)$

iii. Soient $x, y \in \mathbb{Q}_p$

$$\left. \begin{array}{l} x = up^{\nu(x)} \text{ avec } u \text{ unité dans } \mathbb{Z}_p \\ y = vp^{\nu(y)} \text{ avec } v \text{ unité dans } \mathbb{Z}_p \end{array} \right\} x + y = up^{\nu(x)} + vp^{\nu(y)}$$

$x + y = u'p^{\nu(x+y)}$ avec u' unité dans $\mathbb{Z}_p$.

Soit $k = \inf(\nu(x), \nu(y))$ alors $k \leq \nu(x)$ et $k \leq \nu(y)$.

$x + y = p^k(up^{\nu(x)-k} + vp^{\nu(y)-k}) \Rightarrow p^k | x + y \Leftrightarrow \nu(p^k) \leq \nu(x + y)$

D'où, $k \leq \nu(x + y)$, ce qui implique $\inf(\nu(x), \nu(y)) \leq \nu(x + y)$

□

Propriété 9. *Tout $x \in \mathbb{Q}_p$ admet un unique développement de Hensel.*

$$x = \sum_{n \geq n_0} x_n p^n$$

où $0 \leq x_n < p$ et $n_0 \in \mathbb{Z}$. Si $x_{n_0} \neq 0$ alors $n_0 = \nu(x)$.

Proof. Soit $x \in \mathbb{Q}_p$ alors par la propriété(7) x s'écrit sous la forme $x = up^{n_0}$ où $n_0 \in \mathbb{Z}$ et u unité dans $\mathbb{Z}_p$.

Développement de Hensel dans $\mathbb{Z}_p$ implique:

$$u = \sum_{n \geq 0} u_n p^n$$

D'où,

$$u = \sum_{n \geq 0} u_n p^{n+n_0} = p^{n_0} \sum_{n \geq n_0} u_{n+n_0} p^n = p^{n_0} \sum_{n \geq n_0} x_n p^n$$

avec $x_n = u_{n+n_0}$. Alors x_n est unique car u_n est unique.

Si $x_{n_0} \neq 0$ alors $p^{n_0} | x$ ce qui implique $n_0 \leq \nu(x)$

Si $p^{n_0+1} | x$ alors $x_{n_0} = 0$, d'où $\nu(x) < n_0 + 1$

Donc, $\nu(x) = n_0$.

□

2.4 Espace Métrique $\mathbb{Q}_p$

Avant de définir la topologie p-adique sur $\mathbb{Q}_p$, on veut rappeler la notion de valeur absolue sur un corps K .

Definition 5 (Valeur absolue). *Soit K un corps. Une valeur absolue $|\cdot|$ sur K est une application $K \rightarrow \mathbb{R}_+$ avec $x \mapsto |x|$ vérifiant*

$$|x| = 0 \Leftrightarrow x = 0 \tag{1a}$$

$$\forall x, y \in K \quad |xy| = |x| |y| \tag{1b}$$

$$\forall x, y \in K \quad |x + y| \leq |x| + |y| \tag{1c}$$

Definition 6 (Valeur absolue ultra-métrique). Si on remplace (1c) dans la définition précédente par

$$\forall x, y \in K \quad |x + y| \leq \max(|x|, |y|)$$

alors $|\cdot|$ s'appelle valeur absolue ultra-métrique ou non archimédienne.

Definition 7 (Valeur absolue p-adique). La fonction définie sur $\mathbb{Q}$ dans $\mathbb{R}_+$ par $|\cdot|_p : x \rightarrow p^{-\nu_p(x)}$ s'appelle valeur absolue p-adique, où ν_p est l'exposant de p dans la décomposition de x en facteurs premiers.

On va vérifier que $|\cdot|_p$ est une valeur absolue ultra-métrique.

Vérification:

$$|x + y|_p = p^{-\nu_p(x+y)}$$

Or

$$\nu_p(x + y) \geq \inf(\nu_p(x), \nu_p(y)) \Rightarrow -\nu_p(x + y) \leq \sup(-\nu_p(x), -\nu_p(y))$$

D'où:

$$|x + y|_p \leq p^{\sup(-\nu_p(x), -\nu_p(y))} = \sup(p^{-\nu_p(x)}, p^{-\nu_p(y)}) = \sup(|x|_p, |y|_p).$$

Remarque 1. On a défini la valeur absolue p-adique comme suit:

$$|x|_p = p^{-\nu_p(x)}$$

Mais, nous aurions pu la définir comme:

$$|x|_p = a^{-\nu_p(x)} \text{ où } a > 1 \text{ et } a \in \mathbb{R}$$

Definition 8 (Distance). La valeur absolue $|\cdot|$ définie sur K introduit une métrique sur K . La distance entre deux éléments de K dans cette métrique est $d(x, y) = |x - y|$. Comme dans le cas des valeurs absolues ultra-métriques, on peut aussi définir la distance ultra-métrique. On dit qu'une distance d est ultra-métrique lorsqu'elle vérifie l'inégalité $d(x, y) \leq \max(d(x, z), d(y, z))$, $\forall x, y, z \in K$.

Definition 9 (Topologie p-adique). On définit la topologie p-adique par la famille des boules:

$$V_n(a) = \{x \in \mathbb{Q}_p / |x - a| \leq p^{-n}\} = \{x \in \mathbb{Q}_p / \nu(x - a) \geq n\}$$

où $a \in \mathbb{Q}_p$ et $|x| = p^{-\nu(x)}$.

Propriété 10. Toute boule de l'espace métrique $(\mathbb{Q}_p, |\cdot|)$ est à la fois ouverte et fermée.

Proof. Soit $B(a, r)$ une boule ouverte de $\mathbb{Q}_p$ de centre a et rayon r . Il existe $n \in \mathbb{Z}$ tel que $p^n < r \leq p^{n+1}$.

Soit $x \in B(a, r)$, alors

$$|x - a| < r \Rightarrow |x - a| < p^{n+1} \Rightarrow x \in B(a, p^{n+1})$$

Donc $B(a, r) \subset B(a, p^{n+1})$.
 Si $x \in B'(a, p^n)$ alors

$$|x - a| \leq p^n < r \Rightarrow x \in B(a, r)$$

Donc, $B'(a, p^n) \subset B(a, r) \subset B(a, p^{n+1})$.
 Si $x \in B(a, p^{n+1})$ alors

$$\begin{aligned} |x - a| &< p^{n+1} \\ \Rightarrow \nu(x - a) &> -n - 1 \\ \Rightarrow \nu(x - a) &\geq -n \\ \Rightarrow |x - a| &\leq p^{-n} \\ \Rightarrow x &\in B'(a, p^n) \end{aligned}$$

D'où,

$$B'(a, p^n) \subset B(a, r) \subset B(a, p^{n+1}) \subset B'(a, p^n)$$

Donc,

$$B(a, r) = B(a, p^{n+1}) = B'(a, p^n)$$

Donc, $B(a, r)$ est à la fois ouverte et fermée.

Pour une boule fermée $B'(a, r)$, on prend $p^n \leq r < p^{n+1}$ et de même on montre que $B'(a, r) = B'(a, p^n) = B(a, p^{n+1})$. $\square$

2.5 Théorème d'Ostrowski

Nous savons définir sur $\mathbb{Q}$ trois types de valeurs absolues:

- **Valeur absolue triviale:** $|0| = 0$ et $|x| = 1 \forall x \neq 0$
- **Valeur absolue naturelle:** On considère l'application de

$$\begin{aligned} \mathbb{Q} &\longrightarrow \mathbb{Q}_+ \\ x &\longrightarrow |x|_\infty = \sup(x, -x) = \sup(x, 0) - \inf(x, 0) \end{aligned}$$

- **Valeur absolue p-adique:** voir la définition (7).

On se propose maintenant de montrer que les seules valeurs absolues sur $\mathbb{Q}$ sont les valeurs absolues p-adiques et les valeurs absolues $|x|_\infty^\alpha$ où $0 < \alpha \leq 1$.

Theorem 1. *Soit $x \mapsto |x|$ une valeur absolue non triviale sur $\mathbb{Q}$, alors deux cas sont possibles:*

- *S'il existe un entier n tel que $0 < |n| < 1$ alors il existe un nombre premier p tel que $|p| < 1$ et il existe $a \in \mathbb{R}$ $0 < a < 1$ tel que la valeur absolue $|\cdot|$ coïncide avec la valeur absolue p-adique. Autrement dit $|x| = |x|_p = a^{-\nu_p(x)}$*
- *Si pour tout entier n on a $|n| \geq 1$ alors $\exists \alpha \in \mathbb{R}$ tel que $\forall x \in \mathbb{Q}$, $|x| = |x|_\infty^\alpha$ où $0 < \alpha \leq 1$*

Proof. Soit $|\cdot|$ une valeur absolue non-triviale sur $\mathbb{Q}$.

Premier cas: On suppose qu'il existe un entier n tel que $|n| < 1$.

Existence d'un nombre p -adique tel que $|p| < 1$: Supposons par l'absurde que $\forall p$ premier, $|p| \geq 1$. Soit $n \in \mathbb{N}$ tel que $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$ où $p_1 \dots p_k$ sont premiers (décomposition en facteurs premiers). D'après l'axiome (1b) de la valeur absolue, $|n| = |p_1|^{r_1} \cdot \dots \cdot |p_k|^{r_k} \Rightarrow |n| \geq 1$ (car $\forall p$ premier $|p| \geq 1$). Il y a contradiction, donc $\exists p$ premier tel que $|p| < 1$.

Pour la suite de la preuve, nous avons besoin de deux lemmes qui seront démontrés après la démonstration du théorème d'Ostrowski.

Lemme 1. *S'il existe un nombre premier p tel que $|p| < 1$ alors $\forall b \in \mathbb{N}, |b| \leq 1$.*

Lemme 2. *Soit p un nombre premier tel que $|p| < 1$ alors pour tout entier q tel que $(p, q) = 1$, on a $|q| = 1$.*

D'après le lemme 2, p est unique. Alors on prend $a = |p|$. Soit $x \in \mathbb{Q}$, x s'écrit:

$$x = \frac{m}{n} p^{\nu_p(x)} \text{ où } p \nmid m \text{ et } p \nmid n$$

Alors, $(p, m) = 1$ et $(p, n) = 1$.

$$\text{Lemme 2} \Rightarrow |m| = 1 \text{ et } |n| = 1 \Rightarrow \left| \frac{m}{n} \right| = 1|.$$

D'où,

$$|x| = \left| \frac{m}{n} p^{\nu_p(x)} \right| = \left| \frac{m}{n} \right| |p|^{\nu_p(x)} = a^{\nu_p(x)} = |x|_p$$

Deuxième cas: On suppose que $\forall n \in \mathbb{N}, |n| \geq 1$. Alors, il existe $a \in \mathbb{N}$ tel que $|a| > 1$, sinon $|\cdot|$ serait triviale. On pose:

$$|a| = a^\alpha \Rightarrow \alpha = \frac{\log |a|}{\log a}$$

Or, on a $\forall n \in \mathbb{N}, |n| \leq n$ car $|n| = \overbrace{|1 + \dots + 1|}^{(n \text{ fois})} \leq |1| + \dots + |1| = n$ (par l'axiome (iii)), d'où $\log |a| \leq \log a \Rightarrow 0 < \alpha \leq 1$.

Soit $N \in \mathbb{N}$. On écrit la décomposition de N dans la base a alors:

$$N = x_0 + x_1 a + \dots + x_{k-1} a^{k-1} \text{ où } 0 \leq x_i \leq a-1, \quad 1 \leq i \leq k-1 \text{ et } x_{k-1} \neq 0.$$

$$|N| \leq |x_0| + |x_1| |a| + \dots + |x_{k-1}| |a|^{k-1}.$$

On a $\forall i = 1, \dots, k-1, x_i \leq a-1 \Rightarrow |x_i| \leq |a-1| \leq a-1$, d'où

$$\begin{aligned} |N| &\leq (a-1)(1 + |a| + \dots + |a|^{k-1}) \\ &\leq (a-1)(1 + a^\alpha + \dots + a^{\alpha(k-1)}) \\ &\leq (a-1) \frac{a^{\alpha k} - 1}{a^\alpha - 1} < (a-1) \frac{a^{\alpha k}}{a^\alpha - 1} = \frac{a-1}{a^\alpha - 1} a^\alpha a^{\alpha(k-1)} \end{aligned}$$

Or,

$$a^{k-1} \leq N < a^k \Rightarrow a^{\alpha(k-1)} \leq N^\alpha < a^{\alpha k}$$

D'où,

$$|N| \leq \frac{a-1}{a^\alpha - 1} a^\alpha N^\alpha$$

On pose

$$C = \frac{a-1}{a^\alpha-1} a^\alpha \text{ constante indépendante de } N$$

$$\Rightarrow |N| \leq CN^\alpha$$

Soit $m \in \mathbb{N}$. On remplace N par N^m alors;

$$|N^m| = |N|^m \leq CN^{\alpha m} \Rightarrow |N| \leq C^{\frac{1}{m}} N^\alpha$$

On fait tendre m vers $+\infty$ alors

$$|N| \leq N^\alpha$$

L'inégalité dans l'autre sens:

Comme $a^{k-1} \leq N < a^k$, on peut considérer $N = a^k - b$ où $b \in \mathbb{N}$ et $0 < b \leq a^k - a^{k-1}$. $N = a^k - b \Rightarrow |N| \geq |a|^k - |b|$.

On a montré que $\forall x \in \mathbb{N}$, $|x| \leq x^\alpha$ alors $|b| \leq b^\alpha$ d'où

$$|N| \geq |a|^k - b^\alpha \geq |a|^k - (a^k - a^{k-1})^\alpha = a^{\alpha k} - a^{\alpha k} \left(1 - \frac{1}{a}\right)^\alpha$$

$$|N| \geq a^{\alpha k} \left(1 - \left(1 - \frac{1}{a}\right)^\alpha\right)$$

On pose

$$C_1 = \left(1 - \left(1 - \frac{1}{a}\right)^\alpha\right) \text{ constante indépendante de } N$$

$$\Rightarrow |N| \geq a^{\alpha k} C_1$$

Or, $N^\alpha < a^{\alpha k} \Rightarrow |N| > N^\alpha C_1$.

Soit $m \in \mathbb{N}$, on remplace N par N^m alors

$$|N| > N^\alpha C^{\frac{1}{m}}$$

On fait tendre m vers $+\infty$ alors

$$|N| < N^\alpha, \text{ donc } \forall N \in \mathbb{N}, \quad |N| = N^\alpha.$$

Mais $N \in \mathbb{N}$, alors

$$|N|_\infty^\alpha = [\sup(-N, N)]^\alpha = N^\alpha$$

Donc, si $\forall n \in \mathbb{N}$, $|n| \geq 1$ alors

$$\forall N \in \mathbb{N}, \quad |N| = |N|_\infty^\alpha$$

Extention de la conclusion sur $\mathbb{Q}$:

Soit $x \in \mathbb{Q}$, alors x s'écrit

$$x = \frac{N}{N'} \text{ avec } N, N' \in \mathbb{N} \text{ et } N' \neq 0$$

$$|x| = \left| \frac{N}{N'} \right| = \frac{|N|}{|N'|} = \frac{|N|_\infty^\alpha}{|N'|_\infty^\alpha} = \left| \frac{N}{N'} \right|_\infty^\alpha = |x|_\infty^\alpha$$

□

Voici les démonstrations des lemmes:

Démonstration du lemme (1). On suppose qu'il existe un nombre premier p tel que $|p| < 1$. Soit $b \in \mathbb{N}$. On écrit b dans la base p :

$$\begin{aligned} b &= x_0 + x_1p + \dots + x_kp^k \text{ où } 0 \leq x_i \leq p-1, \quad \forall i = 0, \dots, k \text{ et } x_k \neq 0. \\ |b| &\leq |x_0| + |x_1||p| + \dots + |x_k||p|^k \\ &\leq |p-1|(1 + |p| + \dots + |p|^k) \text{ car } |x_i| \leq |p-1| \quad \forall i = 0, \dots, k \\ &\leq |p-1|(1+k) \end{aligned}$$

On passe à la n ème puissance de b et on écrit b^n dans la base p . Dans cette écriture, soit k_n l'indice du dernier des chiffres non nul. Alors,

$$|b^n| = |b|^n \leq |p-1|(1+k_n)$$

mais

$$b^n \geq p^{k_n} \Rightarrow k_n \leq k \frac{\log b}{\log p}.$$

On pose

$$B = \frac{\log b}{\log p}$$

d'où

$$\begin{aligned} |b|^n &\leq |p-1|(1+k_n) \\ \Rightarrow |b| &\leq |p-1|^{\frac{1}{n}}(1+k_n)^{\frac{1}{n}} \end{aligned}$$

On fait tendre n vers $+\infty$ donc $|b| \leq 1$. □

Démonstration du lemme (2). :

On suppose que p est premier tel que $|p| < 1$ et $q \in \mathbb{N}$ tel que $(p, q) = 1$. Soit $n \in \mathbb{N}$, alors p^n et q^n sont encore premiers entre eux.

Alors,

$$\begin{aligned} \exists u_n, v_n \in \mathbb{Z} \text{ tel que } u_np^n + v_nq^n &= 1 \\ \text{Lemme 1} \Rightarrow |u_n| \leq 1, |v_n| \leq 1 \text{ et } |q^n| &\leq 1 \\ \Rightarrow |q| \leq |q^n| &\leq 1 \end{aligned}$$

Supposons par l'absurde que $|q| < 1$. Alors,

$$1 = |1| = |u_np^n + v_nq^n| \leq |u_n||p|^n + |v_n||q|^n \leq |p|^n + |q|^n < 1$$

contradiction. Donc $|q| = 1$. □

2.6 Valeurs absolues équivalentes

Pour voir combien de topologies différentes on peut définir sur $\mathbb{Q}$, nous avons besoin de voir la notion de valeurs absolues équivalentes.

Definition 10. Deux valeurs absolues $|x|_1$ et $|x|_2$ sur un corps K sont dites équivalentes si elles définissent la même topologie. Autrement dit, si d_1 est la distance associée à $|x|_1$ et d_2 la distance associée à $|x|_2$, alors $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes lorsque la famille des boules centrées en un point a définie par d_1 coïncide avec celle définie par d_2 (ou vice-versa) ou encore toute suite de corps K convergente pour $|\cdot|_1$ converge aussi pour $|\cdot|_2$.

Par cette définition et par le théorème d'Ostrowski, on peut conclure qu'on ne peut que définir deux types de topologies sur $\mathbb{Q}$: celle de la valeur absolue ordinaire et celle de la valeur absolue p-adique.

Remarque 2. :

- Pour déduire l'équivalence de deux valeurs absolues, il suffit de considérer que les suites $(x_n)_{n \in \mathbb{N}}$ du corps K sont convergentes vers 0. Finalement, on peut dire que $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes lorsque

$$|x|_1 < 1 \Leftrightarrow |x|_2 < 1.$$

- $B(a, r) = \{x \in K / |x - a| < r\}$. Boule centrée en a de rayon r . Si on prend $|\cdot| = |\cdot|_p$ alors $B(a, r)$ s'écrit:

$$B_n(a) = \{x \in \mathbb{Q}_p / |x - a|_p \leq p^{-n}\} = \{x \in \mathbb{Q}_p / \nu_p(x - a) \geq n\}$$

où $\mathbb{Q}_p$ est le corps de fractions de $\mathbb{Z}_p$.

- Pour la valeur absolue p-adique la suite $(p^n)_{n \in \mathbb{N}}$ converge vers 0 c'est à dire, pour la distance associée à la valeur absolue p-adique notée d , nous avons $d(p^n, 0) \rightarrow 0$. En effet,

$$d(p^n, 0) = |p^n - 0|_p = |p^n|_p = p^{-n} \rightarrow 0$$

Proposition 1. Les valeurs absolues $|x|_1$ et $|x|_2$ sont équivalentes si et seulement si il existe une constante positive c telle que $\forall x \in K$, $|x|_1 = |x|_2^c$

Proof. :

$\Leftarrow$ Supposons que $\exists b > 0$ tel que $|x|_1 = |x|_2^c$ et $|x|_1 < 1$. Alors $|x|_2^c < 1 \Rightarrow |x|_2 < 1$

$\Rightarrow$ On suppose que $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes. Alors on a

$$\forall x \in K, \quad |x|_1 < 1 \Leftrightarrow |x|_2 < 1.$$

$$\text{Soit } \begin{cases} a \in K \setminus \{0\} \text{ tel que } |a|_1 < 1 \\ \text{Soit } b \in K \setminus \{0\} \end{cases} \quad \text{alors } |b|_1 = |a|_1^\alpha$$

$$\text{où } \alpha = \frac{\log|b|_1}{\log|a|_1}, \quad n, m \in \mathbb{N} \text{ et } m \neq 0.$$

Si $\frac{n}{m} > \alpha$ alors $|b|_1 > |a|_1^{\frac{n}{m}} \Rightarrow |b|_1^m > |a|_1^n \Rightarrow \left|\frac{a^n}{a^m}\right|_1 < 1$.

Comme les valeurs absolues sont équivalentes,

$$\left|\frac{a^n}{a^m}\right|_2 < 1 \Rightarrow |b|_2 > |a|_2^{\frac{n}{m}}.$$

Si

$$\frac{n}{m} < \alpha$$

alors par le même raisonnement on obtient:

$$|b|_1 < |a|_1^{\frac{n}{m}} \Rightarrow |b|_2 < |a|_2^{\frac{n}{m}}$$

$$\text{Donc } |b|_2 = |a|_2 \Rightarrow \alpha = \frac{\log |b|_2}{\log |a|_2},$$

$$\text{d'où } \frac{\log |b|_2}{\log |a|_2} = \frac{\log |b|_1}{\log |a|_1} = \alpha \Rightarrow \log |a|_1 = \frac{\log |b|_1 \log |a|_2}{\log |b|_2}$$

$$\text{On pose } c = \frac{\log |b|_1}{\log |b|_2}, \text{ d'où } |a|_1 = |a|_2^c$$

Si a vérifie $|a|_1 > 1$ par le même argument on obtient $|a|_1 = |a|_2^c$ □

Remarque 3. La relation " $|\cdot|_1$ et $|\cdot|_2$ sont deux valeurs absolues équivalentes" est une relation d'équivalence. En effet,

reflexivité: $|\cdot|_1 \sim |\cdot|_1$ car $|x|_1 < 1 \Rightarrow |x|_1 < 1$

symmétrie On suppose $|\cdot|_1 \sim |\cdot|_2$ alors $\exists c > 0$ tel que $|x|_1 = |x|_2^c, \forall x \in K$. Si $|x|_2 < 1$ alors $|x|_2^c < 1 \Rightarrow |x|_1 < 1$ donc $|\cdot|_2 \sim |\cdot|_1$.

transitivité On suppose $|\cdot|_1 \sim |\cdot|_2$ et $|\cdot|_2 \sim |\cdot|_3$ et soit $x \in K$.

$$|\cdot|_1 \sim |\cdot|_2 \Rightarrow (|x|_1 < 1 \Rightarrow |x|_2 < 1)$$

$$|\cdot|_2 \sim |\cdot|_3 \Rightarrow (|x|_2 < 1 \Rightarrow |x|_3 < 1)$$

$$|x|_1 < 1 \Rightarrow |x|_3 < 1$$

$$|\cdot|_1 \sim |\cdot|_3$$

Definition 11. On appelle places du corps K les classes d'équivalences de valeurs absolues.

2.7 Les valeurs absolues sur un corps de nombres

Soit K un corps de nombres de degré n où $n = r + 2s$. Dans ce paragraphe, nous allons voir qu'il y a $r + s$ valeurs absolues non équivalentes de K induisant la topologie réelle (respectivement la topologie p-adique) sur $\mathbb{Q}$.

2.7.1 Valeurs absolues de K qui induisent la topologie réelle sur $\mathbb{Q}$

Definition 12 (Places infinies). On appelle places infinies les classes de valeurs absolues induisant la topologie réelle sur $\mathbb{Q}$.

- Soit f un polynôme irréductible sur $\mathbb{Q}[\mathbb{X}]$ tel que $K = \mathbb{Q}[\mathbb{X}]/f\mathbb{Q}[\mathbb{X}]$

- $\omega : \mathbb{Q}[\mathbb{X}] \mapsto K$
- Soit α_i une racine de f dans $\mathbb{C}$, on lui associe un homomorphisme $p_i : (K, |\cdot|_i) \mapsto (\mathbb{C}, |\cdot|_\infty)$ tel que

$$\begin{cases} p_i(a) = a, \forall a \in \mathbb{Q} \\ p_i(\omega(x)) = \alpha_i \end{cases}$$

où $|\cdot|_\infty$ est module de nombres complexes et p_i est un $\mathbb{Q}$ morphisme. On pose $|x|_i = |p_i(x)|_\infty$. On vérifie immédiatement que $|\cdot|_i$ définit une valeur absolue sur K et elle induit sur $\mathbb{Q}$ la topologie réelle.

- Supposons que f a n racines distinctes dans $\mathbb{C}$, dont r réelles, et $2s$ complexes (avec $n = r + 2s$). Quitte à rénumérer les racines, on peut supposer que les premières r racines sont réelles, $\alpha_{r+1}, \dots, \alpha_{r+s}$ sont complexes dont aucune n'est la conjuguée d'une autre et $\alpha_{r+i} = \overline{\alpha_{r+s+i}}, \forall i \in \{1 \dots s\}$.

Theorem 2. :

- Les $r + s$ valeurs absolues $|x|_i$ (définient comme ci-dessus) sont deux à deux non-équivalentes.
- Soit $|\cdot|$ une valeur absolue quelconque sur K induisant la topologie réelle sur $\mathbb{Q}$, alors $\exists i \in \{1 \dots r + s\}$ tel que $|\cdot|$ et $|\cdot|_i$ soient équivalentes.

Proof. :

- Supposons par l'absurde que $\exists i \neq j \in \{1 \dots r + s\}$ tel que $|x|_i \sim |x|_j$.

$$p_i : K \mapsto \mathbb{C}$$

est continue car

$$K \simeq p_i(K) \subset \mathbb{C}$$

Il est clair que

$$p_i \circ p_j^{-1} : p_j(K) \mapsto p_i(K)$$

est un isomorphisme. On veut montrer que

$$p_i \circ p_j^{-1} : K_j \mapsto K_i$$

est aussi un isomorphisme où

$$K_j = \overline{p_j(K)} = \text{fermeture de } p_j(K)$$

Pour cela, il suffit de montrer que:

- $\forall y \in \overline{p_j(K)}$ tel que $p_i \circ p_j^{-1} = 0 \Rightarrow y = 0$
- $\forall z \in \overline{p_i(K)}, \exists y \in \overline{p_j(K)}$ tel que $p_i \circ p_j^{-1} = z$

- a: Soit $y \in \overline{p_j(K)}$ tel que $p_i \circ p_j^{-1}(y) = 0$. Alors, $\exists (y_n)_{n \geq 0} \in p_j(K)$ tel que $y_n \rightarrow y$ dans $\mathbb{C}$
 $p_i \circ p_j^{-1}$ est continue car p_i et p_j^{-1} sont continues. D'où,

$$\begin{aligned} p_i \circ p_j^{-1}(y_n) &\longrightarrow p_i \circ p_j^{-1}(y) = 0^{(*)} \\ y_n \in p_j(K) &\Rightarrow \exists x_n \in K \text{ tel que } p_j(x_n) = y_n \\ p_i \circ p_j^{-1}(y_n) &= p_i \circ p_j^{-1}(p_j(x_n)) = p_i(x_n) \\ \text{Par } (*) &, p_i(x_n) \longrightarrow 0 \\ &\Rightarrow \text{\`a partir d'un certain rang, } |p_i(x_n)|_\infty = |x_n|_i < 1 \end{aligned}$$

$$\begin{aligned} \text{Or, } |x_n|_i \sim |x_n|_j &\Rightarrow |x_n|_j < 1 \Rightarrow p_j(x_n) \longrightarrow 0 \Rightarrow y_n \longrightarrow 0 \\ \text{L'unicit\'e de la limite} &\Rightarrow y = 0 \end{aligned}$$

- b: Soit $z \in \overline{p_i(K)}$. On cherche $y \in \overline{p_j(K)}$ tel que $p_i \circ p_j^{-1}(y) = z$.
 $z \in \overline{p_i(K)} \Rightarrow \exists (z_n)_{n \geq 0} \in p_i(K)$ tel que $z_n \rightarrow z$ dans $\mathbb{C}$
On prend $y \in p_j(K)$ tel que $y_n \rightarrow y$ dans $\mathbb{C}$ avec $y_n \in p_j(K)$ et $p_i \circ p_j^{-1}(y_n) = z_n$.
La continuit\'e de $p_i \circ p_j^{-1}$ implique $p_i \circ p_j^{-1}(y_n) \rightarrow p_i \circ p_j^{-1}(y)$.
L'unicit\'e de la limite implique $p_i \circ p_j^{-1}(y) = z$.

Donc, $p_i \circ p_j^{-1}$ se prolonge en un isomorphisme de K_j dans K_i .
 K_i et K_j sont complets (car un ferm\'e dans un complet est un complet).
Alors, ils sont soit \u00e9gaux \u00e0 $\mathbb{R}$ ou \u00e0 $\mathbb{C}$.

- Si $K_i = K_j = \mathbb{R}$ alors $p_i \circ p_j^{-1} = Id$ car le seul isomorphisme de $\mathbb{R} \mapsto \mathbb{R}$ est l'identit\'e. D'o\u00f9, $p_i \circ p_j^{-1}(\alpha_j) = \alpha_j = \alpha_i$. Ce qui conredit l'hypoth\ese selon laquelle toutes les racines sont distinctes.
- Si $K_i = K_j = \mathbb{C}$ alors $p_i \circ p_j^{-1}$ est le passage au conjugu\'e donc $\overline{\alpha_j} = \alpha_i$ ce qui est impossible d'apr\es la r\'enum\'eration des racines.

Donc, $\forall i, j \in \{1 \dots r + s\}$, $|x|_i \approx |x|_j$.

- ii. Soit $|x|$ une valeur absolue sur K induisant sur $\mathbb{Q}$ la topologie r\'eelle. On note $\hat{K}$ le compl\'et de K par $|\cdot|$. K est une extension alg\ebrique finie de $\mathbb{Q}$ alors $\hat{K}$ est une extension alg\ebrique de $\mathbb{R}$. Comme $\hat{K}$ est complet et est contenu dans $\mathbb{C}$ il est isomorphe \u00e0 $\mathbb{R}$ ou $\mathbb{C}$. Soit $a : \hat{K} \mapsto \mathbb{C}$ un tel isomorphisme tel que $a(\omega(x)) = \alpha_i$ racine de f alors $p_i \circ a^{-1}$ est l'identit\'e de K . De plus, c'est un hom\'eomorphisme de $(K, |\cdot|)$ sur $(K, |\cdot|_i)$. Donc, $|x| \sim |x|_i$.

□

2.7.2 Valeurs absolues de K qui induisent la topologie p-adique sur $\mathbb{Q}$

Definition 13 (Places finies). On appelle places finies les classes de valeurs absolues induisant la topologie r\'eelle sur $\mathbb{Q}$.

Soit K un corps de nombres et B l'anneau des entiers de K .

Propriété 11. Deux valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ tel que $\{x \in B/|x|_1 < 1\} = \{x \in B/|x|_2 < 1\}$ sont équivalentes.

Proof. Voir le paragraphe précédent. $\square$

Propriété 12. Soit $|x|$ une valeur absolue sur K appartenant à une place finie, alors $B \subseteq \{x \in K/|x| \leq 1\}$.

Proof. Supposons que $|\cdot|$ appartient à une place finie.

Soit $x \in B$ alors $\exists \alpha_1 \dots \alpha_n \in \mathbb{Z}$ tel que:

$$x^n + \alpha_1 x^{n-1} + \dots + \alpha_n = 0 \Rightarrow |x^n| \leq |\alpha_1| |x^{n-1}| + \dots + |\alpha_n|$$

$$\text{Or } \alpha_i \in \mathbb{Z} \Rightarrow \alpha_i \in \mathbb{Q} \Rightarrow |\alpha_i| = |\alpha_i|_p, \forall i \in \{1 \dots n\}$$

Donc, $|\alpha_i| = p^{-\nu_p(\alpha_i)} \leq 1 \Rightarrow |x^n| \leq |x^{n-1}| + \dots + 1 \Rightarrow |x^n| < 2 \Rightarrow |x| \leq 1$ (sinon il existe $k \in \mathbb{N}$ tel que $|x^k| > 2$). $\square$

Propriété 13. Soit $|x|$ une valeur absolue appartenant à une place finie alors $M = \{x \in B/|x| < 1\}$ est un idéal premier de B .

Proof. :

- M est un idéal de B

i. Soient $x, y \in M$ alors $|x| < 1$ et $|y| < 1$. On veut $|x + y| < 1$.

$$\left. \begin{array}{l} |x| < 1 \Leftrightarrow x^n \rightarrow 0 \\ |y| < 1 \Leftrightarrow y^n \rightarrow 0 \end{array} \right\} (x + y)^n \rightarrow 0 \Leftrightarrow |x + y| < 1$$

Donc $x + y \in M$.

ii. Soient $x \in M$ et $b \in B$. On veut $|xb| < 1$. $x \in M \Rightarrow |x| < 1$. D'après la proposition (12), $|b| \leq 1$ d'où $|xb| = |x||b| < 1$. Donc $xb \in M$.

Donc M est un idéal de B .

- M est premier

$$M \text{ premier} \Leftrightarrow \forall x, y \in B \text{ si } xy \in M \text{ alors } x \in M \text{ ou } y \in M$$

$$\Leftrightarrow \forall x, y \in B \text{ si } x \notin M \text{ et } y \notin M \text{ alors } xy \notin M$$

$$\text{Soient } x, y \in B \setminus M \text{ alors } \left\{ \begin{array}{l} |x| \leq 1 \text{ et } |y| \leq 1 \text{ car } x, y \in B \\ |x| > 1 \text{ et } |y| > 1 \text{ car } x, y \notin M \end{array} \right.$$

D'où $|x||y| = |xy| = 1$. Donc $xy \notin M$. $\square$

Definition 14. Soient P un idéal premier de A et $x \in K$.

On dit que $|x|_P = N(P)^{-\nu_P(x)}$ est une valeur absolue P -adique qui induisent sur $\mathbb{Q}$ la topologie p -adique où p est l'unique nombre premier appartenant à P et $\nu_P(x) = n_P(Bx)$.

Remarque 4. :

- On vérifie facilement que $\nu_P(x)$ définit une valuation sur K
- Les valeurs absolues P -adiques appartiennent aux places finies.

Theorem 3. (i) Si P et P' deux idéaux premiers de B tel que $P \neq P'$ alors $|\cdot|_P \approx |\cdot|_{P'}$

(ii) Si $|\cdot|$ est une valeur absolue qui induit la topologie p -adique sur $\mathbb{Q}$ alors il existe P un idéal premier de B tel que $|\cdot| \sim |\cdot|_P$

Proof. (i) Soient P et P' deux idéaux premiers de B tel que $P \neq P'$. Supposons par l'absurde que $|\cdot|_P \sim |\cdot|_{P'}$. D'après la proposition (13), on peut exprimer P sous la forme $P = \{x \in B/|x|_P < 1\}$. Soit $x \in P$ alors $|x|_P < 1$. Comme $|\cdot|_P \sim |\cdot|_{P'}$, on a aussi $|x|_{P'} < 1$, alors $x \in P'$ d'où $P \subset P'$. De même, $P' \subset P$ donc $P = P'$ (contradiction).

(ii) Soit $|\cdot|$ une valeur absolue qui induit la topologie p -adique sur $\mathbb{Q}$. Alors $|\cdot|$ appartient à une place finie. D'après la proposition (13), $|\cdot|$ définit un idéal premier que l'on peut exprimer $P = \{x \in B/|x| < 1\}$. Mais P peut aussi être exprimé sous la forme $\{x \in B/|x|_P < 1\}$. D'où $\{x \in B/|x| < 1\} = \{x \in B/|x|_P < 1\}$. Donc, $|\cdot| \sim |\cdot|_P$. □

A Appendix

A.1 Idéaux Fractionnaires

Definition 15 (Idéal Fractionnaire). Soient A un anneau intègre et K son corps de fractions. On dit que I est un idéal fractionnaire de A lorsque;

- I est un sous A module de K
- $\exists d \in A$ tel que $dI \subset A$

Remarque 5. :

1. La définition d'un idéal fractionnaire est équivalente à dire que les éléments de I ont un dénominateur commun. ($I \subset d^{-1}A$)
2. Tous les idéaux de A sont des idéaux fractionnaires pour $d = 1$. On les appelle les idéaux entiers de A .
3. Tout A module I de K de type fini est un idéal fractionnaire. En fait, supposons que I est engendré par l'ensemble $\{x_1, x_2, \dots, x_n\}$ avec $x_i \in K \quad \forall i \in \{1, \dots, n\}$. On peut écrire $x_i = a_i d_i^{-1}$ avec $a_i, d_i \in A$ et $d_i \neq 0$. On note $d = d_1 \dots d_n$ alors $dI \subset A$.
4. Si A est noethérien alors tout idéal fractionnaire est un A module fini. En fait, soit I un idéal fractionnaire alors I est un sous A module et $\exists d \in A$ tel que $I \subset d^{-1}A$. A est noethérien alors $d^{-1}A$ est noethérien. Donc I est de type fini.

On note $I(A)$ l'ensemble des idéaux fractionnaires non nuls de A et on définit sur cet ensemble l'opération multiplication suivante:

$$I, J \in I(A) \quad IJ = \left\{ \sum_{i=1}^r a_i b_i / r \text{ entier quelconque, } a_i \in I, b_i \in J \right\}$$

Definition 16. Soit $I \in I(A)$. On dit que $J \in I(A)$ est l'inverse de I dans $I(A)$ si $IJ = A$.

Propriété 14. Pour l'opération multiplication définie ci-dessus $I(A)$ est un monoïde.

Proof. :

- Soient $I, J \in I(A)$ alors il exist $d, d' \in A$ tel que $dI \subset A$ et $d'J \subset A$. D'où $dd'IJ \subset A$ donc $IJ \in I(A)$.
- Associativité : évidente
- Élément neutre : A

□

A.2 Anneaux de Dedekind

Definition 17 (Anneau de Dedekind). *A est dit un anneau de Dedekind lorsque;*

- *A est intégralement clos.*
- *A est noethérien.*
- *Tout idéal premier non nul de A est maximal.*

Remarque 6. *Tout anneau principal est un anneau de Dedekind.*

D'après le théorème suivant, on va voir que l'anneau des entiers d'un corps de nombres est un anneau de Dedekind.

Theorem 4. *Soient A un anneau de Dedekind, K son corps de fractions, L une extension de degré finie de K et A' la fermeture intégrale de A dans L. On suppose K de caractéristique 0. Alors A' est un anneau de Dedekind et un A module de type fini.*

Proof. On veut montrer que A' est un anneau de Dedekind, c'est-à-dire intégralement clos, noethérien et tout idéal premier de A' est maximal.

i *A' est intégralement clos*
Par construction, A' est intégralement clos.

ii *A' est noethérien*
A' est noethérien grâce à la proposition suivante:

Proposition 2. *Soient A un anneau noethérien intégralement clos, K son corps de fractions, L une extension de degré fini de n de K et A' la fermeture intégrale de A dans L. On suppose K de caractéristique 0. Alors A' est un A module de type fini et un anneau noethérien.*

iii *Tout idéal premier non nul de A' est maximal*

Soit P' un idéal premier non nul de A'.

Soit $x \in P' \subset A'$ tel que $x \neq 0$ alors x est entier sur A.

Il existe $\{a_0, \dots, a_{n-1}\} \in A$ tel que (*) $x^n + a_{n-1}x^{n-1} + \dots + a_1 = 0$.

Supposons que cette équation est de degré minimum alors $a_0 \neq 0$ (sinon, on aura $x^{n-1} + a_{n-1}x^{n-1} + \dots + a_1 = 0$ ce qui contredit la minimalité du degré de (*)).

$a_0 = -x^n - a_{n-1}x^{n-1} - \dots - a_1x \Rightarrow a_0 \in xA \subset P'$ (car P' est un idéal)

$\Rightarrow a_0 \in xA \cap A \subset P' \cap A \Rightarrow P' \cap A \neq \emptyset$

Or $P' \cap A$ est un idéal premier de A.

Comme A est noethérien, $P' \cap A$ est un idéal maximal de A ceux qui implique $A/P' \cap A$ est un corps et on conclut avec le lemme suivant qui sera démontré juste après cette preuve:

Lemme 3. *Avec les notations du théorème;*

a- *Soit A' est intègre alors*

$A' \text{ est un corps} \Leftrightarrow A \text{ est un corps.}$

b- Soit P' est un idéal premier de A' alors

P' est un idéal maximal de $A' \Leftrightarrow P' \cap A$ est un idéal maximal de A

□

Preuve du lemme 3. :

a- $\Rightarrow$ On suppose que A' est un corps. Soit $x \in A$ non nul.

Comme $A \subset A'$ on a $x \in A'$.

A' est un corps alors $x^{-1} \in A'$ donc x^{-1} est un entier sur A .

Il existe $\{a_1, \dots, a_n\} \in A$ tel que $(x^{-1})^n + a_1(x^{-1})^{n-1} + \dots + a_n = 0 \Rightarrow x^{-1} + a_1 + \dots + a_n x^{n-1} = 0 \Rightarrow x^{-1} = -a_1 - \dots - a_n x^{n-1} \in A$

donc A est un corps.

$\Leftarrow$ On suppose que A est un corps. Soit $x \in A'$ non nul.

x est un entier sur A alors il exist $\{\alpha_1, \dots, \alpha_n\} \in A$ tel que

$$\begin{aligned} x^n + \alpha_1 x^{n-1} + \dots + \alpha_n &= 0 \\ \Rightarrow x^n + \alpha_1 x^{n-1} + \dots + \alpha_{n-1} &= -\alpha_n \\ \Rightarrow x(x^{n-1} + \alpha_1 x^{n-2} + \dots + \alpha_{n-1}) &= -\alpha_n \end{aligned}$$

On peut supposer que $\alpha_n \neq 0$ car si $\alpha_n = 0$ alors

$$x(x^{n-1} + \alpha_1 x^{n-2} + \dots + \alpha_{n-1}) = 0$$

et comme A est intègre on a soit $x = 0$ soit

$$x^{n-1} + \alpha_1 x^{n-2} + \dots + \alpha_{n-1} = 0$$

mais x est non nul par hypothèse donc on recommence avec

$$x^{n-1} + \alpha_1 x^{n-2} + \dots + \alpha_{n-1} = 0.$$

D'où

$$x(-\alpha_n^{-1} x^{n-1} - \alpha_n^{-1} \alpha_1 x^{n-2} - \dots - \alpha_n^{-1} \alpha_{n-1}) = 1$$

Donc A' est un corp.

Remarque 7. B entier sur A et P idéal de A alors B/P entier sur $A/P \cap A$

b- Soit P' un idéal premier dans A' alors A'/P' est intègre.

D'après a- et la remarque on a b-.

□

Preuve de la Proposition 2. : On va prouver cette proposition à partir d'un théorème et d'un corollaire qui sont les suivants:

Theorem 5. Soient A un anneau intègralement clos, K son corps de fraction, L une extension de K de degré n . On pose A' fermeture intégrale de A sur L . Alors A' est un sous A module d'un A module libre de rang n

Corollaire 1. Si on suppose les hypothèses du théorème précédent et plus A principal alors A' est un A module libre.

A' vérifie les hypothèses du théorème (5) donc A' est un sous A module d'un A module de rang n . De plus comme A est noethérien il est aussi principal alors (1) implique A' est un A module libre. Donc A' est de type fini et noethérien. $\square$

Preuve du théorème (5). :

$$A' = \{x \in L/x \text{ entier sur } A\}$$

On a $[L : K] = n$ alors il existe $(x_1, \dots, x_n)$ une base de L sur K .

$\forall i \in \{1, \dots, n\}$, x_i est algébrique sur K car chaque extension fini est algébrique.

Il existe $\{a_1, \dots, a_n\} \in A$ tel que $a_n x_i^{n-1} + \dots + a_0 = 0$.

Alors $a_n + a_{n-1} x_i^{-1} + \dots + a_0 x_i = 0$.

Par le même raisonnement que l'on a fait dans le lemme (3), on peut supposer que $a_n \neq 0$.

En multipliant par a_n^{n-1}

$$a_n^n + a_n^{n-1} a_{n-1} x_i^{-1} + \dots + a_n^{n-1} a_0 x_i^{-n} = 0$$

$$(a_n x_i)^n + a_{n-1} (a_n x_i^{-1})^{n-1} + \dots + a_0 a_n^{n-1} = 0$$

donc $a_n x_i$ est un entier sur A .

On pose $a_n x_i = x'_i$. $x'_i \in L$, $\forall i \in \{1, \dots, n\}$

Comme x'_i est un entier sur A , $x'_i \in A'$ alors $\{x'_1, \dots, x'_n\}$ est une base de L sur K contenu dans A .

Donc L a deux bases $\mathbf{B}_1 = (x_1, \dots, x_n)$ et $\mathbf{B}_2 = (x'_1, \dots, x'_n)$.

Soit $z \in A' \subset L$ alors z s'écrit

$$z = \sum_{i=1}^n b_j x_j \text{ avec } b_j \in K$$

$\forall i$, $x_i z \in A'$ alors $Tr(x'_i z) \in A$.

$$Tr(x'_i z) = Tr\left(\sum_{j=1}^n b_j x_j, x'_i\right) = \sum_{j=1}^n b_j Tr(x_j, x'_i) = \sum_{j=1}^n b_j \delta_{ij} = b_i \in A$$

$$\text{Alors } z \in \sum_{i=1}^n A x_i.$$

Donc A' est contenu dans un A module libre de rang n . $\square$

Preuve du corollaire (1). : D'après le théorème (5), A' est un sous A module d'un A module libre de rang n . On a aussi A principal, donc d'après le théorème des diviseurs élémentaires (vu en cours), A' est un sous A module libre de rang $\leq n$. Or pendant la preuve du théorème (5), on a vu que A' contient une base de L donc A' est un A module libre de rang n . $\square$

Theorem 6. Soit A un anneau de Dedekind qui n'est pas un corps. Tout idéal maximal de A est inversible dans $I(A)$.

Proof. Soit M un idéal maximal de A . A n'est pas un corps alors $M \neq (0)$. On pose $M' = \{x \in K/xM \subset A\}$. On va montrer que $M' \in I(A)$ et $M'M = A$.

a- $M' \in I(A)$

- a_1 - Soient $x, y \in M'$ alors $xM' \subset A$ et $yM' \subset A$. D'où $xMyM = xyM \subset A$.
 Soient $x, y \in M'$ et $\alpha, \beta \in A$ alors $(x\alpha + y\beta)M \subset A$.
 Donc M' est un sous A module de K .
- a_2 - On cherche $d \in A$ tel que $dM' \subset A$, c'est à dire $\forall x \in M'$ on a $dx \in A$
 Soit $x \in M'$ alors $xM \subset A$.
 On prend $d = m$ où $m \in M \subset A$ quelconque. Donc $dM' \subset A$.

Donc M' est un idéal fractionnaire de A .

b- $\underline{M'M = A}$ On va le montrer par double inclusion.

- $\subset$: Il est clair que $M'M \subset A$
- $\supset$: On a toujours $A \subset M'$. En fait; $\forall a \in A \quad aM \subset M \subset A$ (car M est un idéal de A), donc $a \in M'$.
 Alors $AM = M \subset M'M \subset A$ ce qui implique que $M'M$ est un idéal entier de A . Mais M est l'idéal maximal de A , donc ou bien $M'M = A$ ou bien $M'M = M$. Si $M'M = A$, on aura prouvé le théorème. Alors montrons que $M'M \neq M$.
 Supposons, par l'absurde, que $M'M = M$ et montrons que $M' = A$.
 On a toujours $A \subset M'$.
 Soit $x \in M'$ alors $xM \subset M$ et par récurrence,

$$\forall n \in \mathbb{N} \quad x^n M \subset M \subset A \quad A[x] = \{g(x)/g \in A[X]\} \Rightarrow A[x]M \subset A$$

alors $A[x]$ est un idéal fractionnaire. Or A noethérien implique que $A[x]$ est un sous A module de type fini (Rappel: Théorème de la théorie de Galois: $x \in B$ entier sur $A \Leftrightarrow A[x] \subset B$ est un A module de type fini). Donc, x entier sur A , or A est un anneau de Dedekind ce qui implique A est intégralement clos donc $x \in A$. Donc $M' \subset A$. On a montré que si $M'M = M$ alors $M' = A$.

Or, $M' = A$ est impossible car; soit $a \in M$ non nul. (a) contient un produit $P_1 \dots P_n$ d'idéaux premiers non nuls. On peut supposer n minimum. On a $M \supset (a) \supset P_1 \dots P_n \Leftrightarrow M$ contient au moins l'un des P_i . Disons M contient P_1 . P_1 est un idéal premier non nul de A et A est un anneau de Dedekind. Donc P_1 est un idéal maximal. Donc, $M = P_1$. $(a) \supset P_1 P_2 \dots P_n$ et $(a) \not\supset P_2 \dots P_n$ (car n minimal). $\exists b \in P_2 \dots P_n$ tel que $b \notin (a)$. $P_1 b \subset (a) \Rightarrow P_1 b a^{-1} \subset A$. Définition de $M' \Rightarrow b a^{-1} \in M'$. Mais $b \notin (a) \Rightarrow b a^{-1} \notin A$. Donc $A \neq M'$.

Donc $M'M = A$.

□

Theorem 7. Soient A un anneau de Dedekind, $\mathbf{P}$ l'ensemble des idéaux premiers non nuls de A . Alors

- a- Tout idéal fractionnaire non nul I de A s'écrit, d'une façon et d'une seule, sous la forme

$$I = \prod_{P \in \mathbf{P}} P^{n_P(I)}$$

où les $n_P(b)$ sont des entiers relatifs, presque tous nuls.

b- Le monoïde des idéaux fractionnaires non nuls de A est un groupe.

Proof. :

a_1 - Existence de l'écriture

Soit I un idéal fractionnaire non nul de A , alors il existe $d \in A$ non nul tel que $(dI) \subset A$. D'où (dI) est un idéal entier de A et $I = (dI)(dA)^{-1}$. Autrement dit I s'écrit en tant que produit de deux idéaux entiers de A . Alors il suffit de montrer l'existence de l'écriture pour un idéal entier de A .

On considère l'ensemble ϕ des idéaux de A qui ne sont pas produits d'idéaux premiers. On veut montrer que ϕ est vide.

Supposons, par l'absurde, que $\phi \neq \emptyset$. A est noethérien, alors ϕ admet un idéal maximal noté (a) . (a) est un idéal non nul de A tel que (a) ne s'écrit pas comme produit des idéaux premiers et $\forall I \in \phi \quad I \subset (a)$. On remarque d'abord que $(a) \neq A$ car A est produit de la famille libre d'idéaux premiers. D'après le théorème de Krull, qui dit que tout idéal est contenu dans un idéal maximal, il exist P idéal maximal de A tel que $(a) \subset P$. Mais A est un anneau de Dedekind donc P est premier. Théorème (6) implique P admet un inverse dans $I(A)$ que l'on note P^{-1} .

$$(a) \subset P \Rightarrow (a)P^{-1} \subset PP^{-1} = A$$

Comme $A \subset P^{-1}$, on a

$$(a) \subset (a)P^{-1} \text{ et } (a) \neq (a)P^{-1}$$

En fait, si on a

$$(a)P^{-1} = a \text{ et } x \in P^{-1}$$

alors

$$x(a) \subset (a) \Rightarrow \forall n \quad x^n(a) \subset (a)$$

or (a) est maximum de ϕ donc

$$(a)P^{-1} \notin \phi$$

Donc, $(a)P^{-1}$ est produit des idéaux premiers non nuls. D'où $(a)P^{-1}$ s'écrit

$$(a)P^{-1} = P_1 \dots P_n \text{ où les } P_i \text{ sont dans } \mathbf{P}$$

$$(a) = PP_1 \dots P_n$$

Ainsi, tout idéal entier de A est produit des idéaux premiers de A . D'où l'existence.

a_2 - Unicité de l'écriture

Soit I un idéal fractionnaire de A .

$$I = \prod_{P \in \mathbf{P}} P^{n_P} = \prod_{P \in \mathbf{P}} P^{m_P} \Rightarrow \prod_{P \in \mathbf{P}} P^{n_P - m_P} = A$$

On suppose qu'il existe $P \in \mathbf{P}$ tel que $n_P \neq m_P$ (sinon on aura l'unicité). On sépare les exposants positifs et négatifs alors

$$P_1^{\alpha_1} \dots P_r^{\alpha_r} = Q_1^{\beta_1} \dots Q_s^{\beta_s}$$

P_1 contient $Q_1^{\beta_1} \dots Q_s^{\beta_s} \Rightarrow P_1$ contient l'un des Q_j . Disons P_1 contient Q_1 comme P_1 et Q_1 sont maximaux $P_1 = Q_1$ contradiction d'où l'unicité.

□

A.3 Norme d'un Idéal

Dans ce paragraphe, K désigne un corps de nombres de degré n et A l'anneau des entiers de K .

Proposition 3. *Si $x \in A$ non nul alors $|N(x)| = \text{card}(A/Ax)$.*

Proof. On a vu qu'un anneau des entiers est un anneau de Dedekind alors tous les idéaux premiers non nuls de A sont maximaux. D'après le théorème de cours, qui dit que A est un anneau principal si et seulement si tous les idéaux premiers sont maximaux, A est principal. Le théorème (5) et le corollaire (1) impliquent A est $\mathbb{Z}$ module libre de rang n . On considère l'application:

$$\begin{aligned} L_x : A &\mapsto Ax \\ a &\mapsto ax \end{aligned}$$

C'est un isomorphisme alors Ax est un sous $\mathbb{Z}$ module de A de rang n . Le théorème des diviseurs élémentaires implique qu'il existe une base de A $(e_1, \dots, e_n)$ et il existe $(c_1 \dots c_n) \in \mathbb{Z}$ tel que $c_1|c_2|\dots|c_n$ et $(c_1e_1, \dots, c_n e_n)$ est une base de Ax . Alors;

$$A/Ax \cong \prod_{i=1}^n \mathbb{Z}/c_i\mathbb{Z}$$

Donc $\text{card}(A/Ax) = c_1 \dots c_n$.

Par définition, $N(x)$ est le déterminant de l'application multiplication par x . On définit les applications suivantes:

$$\begin{aligned} u : A &\mapsto Ax \text{ tel que } u(e_i) = c_i e_i, \forall i \in 1, \dots, n \\ v : Ax &\mapsto Ax \text{ tel que } v(c_i e_i) = x e_i, \forall i \in 1, \dots, n \end{aligned}$$

Il est clair que leur composé est l'application multiplication par x . Alors

$$N(x) = \det(v \circ u) = \det(v)\det(u) = \pm c_1 \dots c_n$$

d'où la proposition. □

Remarque 8 (Remarque et rappel). :

- Si $x \in A$ alors x est entier sur A car A est intégralement clos. Donc, $N(x) \in \mathbb{Z}$ (car A est un $\mathbb{Z}$ module).
- Si $I \subset J \subset A$ alors $A/J \cong A/I/J/I$ et $\text{card}(A/J) = \frac{\text{card}(A/I)}{\text{card}(J/I)}$.
- $N(x) = \det|u_x|$ où u est un endomorphisme multiplication par x .

Definition 18. Soit I un idéal non nul de A . On appelle norme de I le nombre $\text{card}(A/I)$ et on le note $N(I)$.

Remarque 9. :

- $N(I)$ est toujours fini. En effet comme I non nul, il existe $x \in I$ non nul alors

$$(x) \subset I \subset A \Rightarrow A/I \subset A/(x) \Rightarrow N(I) = \text{card}(A/I) \leq \text{card}(A/(x))$$

La proposition (3) implique $\text{card}(A/(x))$ est fini d'où $N(I)$ est fini.

- Si I est principal alors $N(I) = |N(x)|$ où $(x) = I$.

Proposition 4. Soient I, J deux idéaux entiers non nuls de A alors $N(IJ) = N(I)N(J)$.

Proof. D'après le théorème (7) I (ou J) s'écrit

$$I = \prod_{P \in \mathbf{P}} P^{n_P(I)} \text{ où } \mathbf{P} \text{ est l'ensemble des idéaux premiers non nuls de } A.$$

Comme A est un anneau de Dedekind, les éléments de $\mathbf{P}$ sont maximaux. Alors il suffit de montrer que $N(PJ) = N(P)N(J)$ avec P idéal maximal de A .

$$\begin{aligned} JA &\subset J \\ \Rightarrow JP &\subset J \subset A \\ \Rightarrow A/JP &/ J/JP \cong A/J \\ \Rightarrow \text{card}(A/JP) &= \text{card}(A/J)\text{card}(J/JP) \end{aligned}$$

Il reste à montrer que $\text{card}(J/JP) = \text{card}(A/P)$.

J est un A module. P est un idéal maximal de A . Alors J/JP est un A/P espace vectoriel. On doit montrer que $\dim(J/JP) = 1$ sur A/P . Les sous espaces vectoriels de J/JP sont de la forme J'/JP où J' est un idéal entier de A et $JP \subset J' \subset J$. Le théorème (7) implique:

$$J = \prod_{P \in \mathbf{P}} P^{n_P} \Rightarrow JP = \prod_{P \in \mathbf{P}} P^{n_P+1}$$

On ne peut pas trouver un idéal J' strictement coïncé entre ces deux produits. D'où, $\dim(J/JP) = 1$ sur A/P . Donc $\text{card}(J/JP) = \text{card}(A/P)$. $\square$

B Bibliographie

Les nombres p-adiques, Yvette Amice, Collection Sup

Théorie algébrique des nombres, Pierre Samuel, Collection Méthodes

Cours d'algèbre, J. Querré, Masson

Introduction to p-adic numbers and valuation theory, George Bachman, Academic Press